

# TRAITE DE COOPERATION EN MATIERE DE BREVETS

**PCT**

## NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents  
United States Patent and Trademark  
Office  
Box PCT  
Washington, D.C.20231  
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

<b>Date d'expédition (jour/mois/année)</b> 20 octobre 2000 (20.10.00)	<b>Référence du dossier du déposant ou du mandataire</b> 76.0569
<b>Demande internationale no</b> PCT/FR00/00679	<b>Date de priorité (jour/mois/année)</b> 17 mars 1999 (17.03.99)
<b>Date du dépôt international (jour/mois/année)</b> 17 mars 2000 (17.03.00)	
<b>Déposant</b> FAUSSE, Arnaud	

1. L'office désigné est avisé de son élection qui a été faite:

☒

dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

08 septembre 2000 (08.09.00)

☐

dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection

☒

a été faite

☐

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI  
34, chemin des Colombettes  
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

R. Forax

no de téléphone: (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

091986645  
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 76.0569	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/00679	International filing date (day/month/year) 17 March 2000 (17.03.00)	Priority date (day/month/year) 17 March 1999 (17.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant SCHLUMBERGER SYSTEMES		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.  
☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of \_\_\_\_\_ sheets.

RECEIVED

FEB 12 2002

Technology Center 2600

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 08 September 2000 (08.09.00)	Date of completion of this report 02 July 2001 (02.07.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00679

## I. Basis of the report

1. With regard to the **elements** of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
pages 1-12, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the claims:  
pages 1-6, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the drawings:  
pages 1/2,2/2, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/FR 00/00679

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Claims	1-6	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-6	NO
Industrial applicability (IA)	Claims	1-6	YES
	Claims		NO

### 2. Citations and explanations

1. The following document is referred to:

D1: WO-A-99/08415.

2. D1 (see page 2, lines 22-34, and page 4, lines 4-16) discloses a method for verifying a message signature which addresses the same problem as the method of the present application, i.e. to prevent tampering with signed data.

In D1, the solution to this problem is based on the same concept as the present Claim 1, namely visual inspection of the said data.

Claim 1 contains certain features which relate to the technical implementation of that basic concept but which in themselves have no particular effect. Consequently, although the subject matter of independent Claim 1 is novel, it is not considered to be inventive.

3. The subject matter of Claims 2-6, which are dependent on Claim 1, is likewise novel. However, these claims contain no additional features that render their subject matter inventive.

**THIS PAGE BLANK (USPTO)**



**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

1. Contrary to the requirements of PCT Rule 5.1(a)(ii), neither D1 nor the relevant prior art disclosed in that document is mentioned in the description.
2. Independent Claim 1 is not correctly drafted in the two-part form (PCT Rule 6.3(b)): features known in combination from prior art (D1) should be mentioned in the preamble (PCT Rule 6.3(b)(i)), and the remaining features should appear in the characterising part (PCT Rule 6.3(b)(ii)).

**THIS PAGE BLANK (USPTO)**

# TRAITE DE COOPERATION EN MATIERE DE BREVETS

## PCT

REC'D 03 JUL 2001

### RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL PCT

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire 76.0569 PCT	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00679	Date du dépôt international (jour/mois/année) 17/03/2000	Date de priorité (jour/mois/année) 17/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant SCHLUMBERGER SYSTEMES et al.		

- Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
- Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.
  - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

- Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 08/09/2000	Date d'achèvement du présent rapport 02.07.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé  Zucka, G  N° de téléphone +31 70 340 4026 

**THIS PAGE BLANK (USPTO)**

# RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00679

## I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

### Description, pages:

1-12                      version initiale

### Revendications, N°:

1-6                      version initiale

### Dessins, feuilles:

1/2-2/2                  version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

**THIS PAGE BLANK** (USPTO)

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00679

- ☐ de la description, pages :  
☐ des revendications, n° :  
☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

*(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)*

6. Observations complémentaires, le cas échéant :

**V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

**1. Déclaration**

Nouveauté	Oui : Revendications 1-6 Non : Revendications
Activité inventive	Oui : Revendications Non : Revendications 1-6
Possibilité d'application industrielle	Oui : Revendications 1-6 Non : Revendications

**2. Citations et explications  
voir feuille séparée**

**VII. Irrégularités dans la demande internationale**

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :  
**voir feuille séparée**

**THIS PAGE BLANK (USPTO)**



**Concernant le point V**

1. Il est fait référence au document suivant:

**D1: WO 99 08415 A**

2. Le document D1 divulgue (voir page 2, lignes 22-34 et page 4, lignes 4-16) un procédé de vérification de signature d'un message, qui tend à résoudre le même problème que le procédé de la présente demande, c.-à-d. d'éviter la manipulation de données signées.

Dans ce document, ledit problème est résolu en se basant sur le même principe que la présente revendication 1, c.-à-d. en effectuant une inspection visuelle des dites données.

La revendication 1 contient certaines caractéristiques qui ont trait à l'implémentation technique de ce principe de base, mais qui en elles-mêmes ne produisent aucun effet particulier. Donc, malgré que l'objet de la revendication indépendant 1 soit nouveau, il n'est pas considéré comme inventif.

3. L'objet des revendications 2-6, qui dépendent de la revendication 1, est également nouveau. Cependant, ces revendications ne contiennent pas d'éléments additionnels qui rendent inventif leur objet.

**Concernant le point VII**

1. Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document D1 et ne cite pas ce document.
2. La revendication indépendante 1 n'est pas présentée dans une forme en deux parties correcte (règle 6.3 b) PCT), les caractéristiques connues en combinaison de l'état de la technique (document D1) figurant dans le préambule (règle 6.3 b) i) PCT) et les caractéristiques restantes figurant dans la partie caractérisante (règle 6.3 b) ii) PCT).

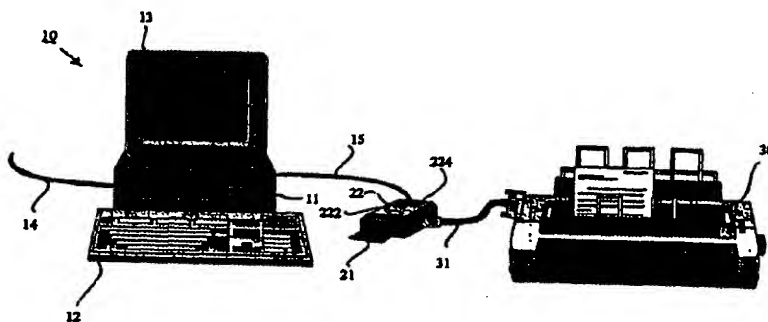
**THIS PAGE BLANK (USPTO)**

## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

<b>(51) Classification internationale des brevets <sup>7</sup> :</b> <b>H04L 9/32</b>	<b>A1</b>	<b>(11) Numéro de publication internationale:</b> <b>WO 00/56007</b> <b>(43) Date de publication internationale:</b> 21 septembre 2000 (21.09.00)
<b>(21) Numéro de la demande internationale:</b> PCT/FR00/00679 <b>(22) Date de dépôt international:</b> 17 mars 2000 (17.03.00) <b>(30) Données relatives à la priorité:</b> 99/03330 ✓ 17 mars 1999 (17.03.99) <b>FR</b> <b>(71) Déposant (pour tous les Etats désignés sauf US):</b> SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR). <b>(72) Inventeur; et</b> <b>(75) Inventeur/Déposant (US seulement):</b> FAUSSE, Arnaud [FR/FR]; 11bis, rue de Maubeuge, F-75009 Paris (FR). <b>(74) Mandataire:</b> UTZMANN-NORTH, Anne; Schlumberger Systèmes, Test & Transactions, 50, avenue Jean Jaurès, Boîte postale 620-12, F-92542 Montrouge Cedex (FR).		<b>(81) Etats désignés:</b> CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Publiée</b> <i>Avec rapport de recherche internationale.</i>

**(54) Title:** METHOD FOR VERIFYING A MESSAGE SIGNATURE**(54) Titre:** PROCEDE DE VERIFICATION DE SIGNATURE D'UN MESSAGE**(57) Abstract**

The invention concerns a method for verifying a message signature, the message, the signature, and a certificate having been sent by a signatory having a public key to an addressee having means (11) for storing messages. The invention is characterised in that it comprises the following steps which consist in: verifying the certificate, in the security means (21) connected to said storage means (11) of the addressee, and transmitting to display means (30) directly connected to the security means (21) at least a result information of verification; verifying the result information on the display means (30); after the certificate has been verified, calculating in the security means (21) a reduction of the message, and copying anew the message on the display means (30) as the reduction operation progresses; decrypting in said security means (21) the signature and the public key of the signatory; comparing the decrypted signature with the reduction performed; depending on the result of the comparison, sending a message, from the security means (21) to the display means (30), indicating whether or not the signature matches the message or the public key and signatory presented. The invention is useful for making secure exchanges on communication networks.



(57) Abrégé

Procédé de vérification de signature d'un message, le message, la signature, et un certificat ayant été envoyés par un signataire possédant une clef publique à un destinataire possédant un moyen (11) de stockage de message. Selon l'invention, ledit procédé comporte les étapes selon lesquelles: on vérifie le certificat, dans le moyen sécurisé (21) connecté audit moyen de stockage (11) du destinataire, et on transmet à un moyen (30) de visualisation connecté directement au moyen sécurisé (21) au moins une donnée de résultat de vérification; on vérifie la donnée de résultat sur le moyen de visualisation (30); lorsque le certificat est vérifié, on calcule dans le moyen sécurisé (21) une réduction du message, et on recopie le message sur le moyen (30) de visualisation au fur et à mesure de l'opération de réduction; on déchiffre dans ledit moyen sécurisé (21) la signature avec la clé publique du signataire; et on compare la signature déchiffrée avec la réduction effectuée; selon le résultat de la comparaison, on envoie un message, du moyen sécurisé (21) au moyen de visualisation (30), indiquant que la signature est conforme ou non au message ou à la clé publique du signataire présentés. Application à la sécurisation des échanges sur les réseaux de communication.

**UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

## PROCEDE DE VERIFICATION DE SIGNATURE D'UN MESSAGE

La présente invention concerne un procédé de vérification de  
5 signature d'un message.

L'invention trouve une application particulièrement avantageuse dans le domaine des télécommunications par transmission de messages sous forme de fichiers électroniques.

Le développement des télécommunications par échange à distance  
10 de fichiers électroniques (commerce électronique, courrier électronique, notariation sous format électronique, etc) a provoqué l'avènement des technologies de traitement cryptographique dont le but est de sécuriser les messages transmis sur les réseaux de communication électronique face notamment aux attaques frauduleuses dont ils peuvent faire  
15 l'objet.

Parmi des opérations de traitement cryptographique d'un message, on peut citer le cryptage du message lui-même, dans sa totalité. Cependant, cette technique reste très lourde et souvent superflue, au moins dans les situations où le destinataire du message souhaite  
20 seulement s'assurer de l'identité de l'expéditeur et de l'intégrité du message qu'il reçoit en clair. C'est pour répondre à ces besoins qu'à été développé le concept de la signature électronique.

La signature électronique repose sur les principes suivants :

- L'auteur d'un message qui souhaite en authentifier l'origine, c'est-  
25 à-dire le signer, dispose d'un nombre secret, appelé clé privée Kpr, destiné à élaborer une signature électronique pour ledit message. Une autre clé, dite clé publique Kpu, est disponible à tout destinataire d'un message en provenance du même expéditeur de manière à pouvoir vérifier la signature électronique du message reçu. Ladite clé publique  
30 est généralement associée au nom de l'expéditeur et à d'autres données, durée de validité de la clé par exemple, dans une structure sécurisée appelée certificat. La sécurisation du certificat repose sur le fait que

l'ensemble des données est lui-même signé par un « tiers de confiance » avec sa clé privée Kprtc et dont la clé publique Kputc est accessible à tous.

5 - L'élaboration de la signature se déroule en deux étapes. Tout d'abord, le message est réduit, on dit aussi « haché », au moyen d'un algorithme de réduction à sens unique, tels que ceux connus sous les noms de SHA1 ou MD5. Ensuite, le message ainsi réduit est crypté par un algorithme à clé publique, RSA, ECC par exemple, au moyen de la clé privée du signataire. Le résultat de ce cryptage constitue la  
10 signature.

- Le message en clair, la signature et, éventuellement, le certificat contenant la clé publique Kpu, sont envoyés au destinataire à travers le réseau de communication.

15 - Le destinataire doit alors vérifier que la signature reçue correspond bien au message et à son auteur. Pour cela, il réduit le message au moyen de l'algorithme de réduction à sens unique choisi par le signataire et décrypte la signature en utilisant la clé publique Kpu du signataire. La signature est reconnue valide si le résultat de la réduction du message est égal au résultat du décryptage de la signature. Le même  
20 procédé peut être utilisé pour vérifier les données contenues dans le certificat à l'aide de la clé publique Kputc du tiers de confiance qui l'a émis.

Il est intéressant de noter que la signature électronique est fonction du contenu du message et de la clé privée du signataire alors  
25 que la signature manuscrite identifie l'auteur mais est indépendante du message.

Afin de donner une valeur légale à la signature électronique, il est nécessaire de prouver certains faits. Entre autres :

- 30 - Le signataire doit disposer d'une clé privée dont personne d'autre ne dispose ;
- Le signataire doit être sûr du message qu'il signe ;

- Le destinataire doit être sûr que la vérification de signature est bien effectuée sur le message reçu ;
- Le destinataire doit être sûr du résultat de la vérification.

Si l'une des conditions ci-dessus n'est pas vérifiée, le signataire  
5 et/ou le destinataire peuvent contester la validité de la signature.

Or, la plupart des opérations de traitement cryptographique d'un message, notamment l'élaboration d'une signature électronique et sa vérification, sont effectuées dans les environnements informatiques de bureau. Cependant, les ordinateurs sont des systèmes ouverts sur  
10 lesquels il n'y a aucun contrôle de la sécurité, car l'utilisateur est libre d'installer tout logiciel de son choix. De même, pour les ordinateurs connectés aux réseaux de communication, de nombreux « virus » ou programmes non souhaitables peuvent être introduits à l'insu de l'utilisateur.

15 Il faut donc considérer l'environnement de l'ordinateur comme étant « non sûr ».

La situation la plus simple pour calculer une signature électronique, par exemple, pourrait consister à utiliser l'ordinateur comme moyen de stockage du message et des clés, et comme moyen  
20 d'élaboration de la signature. Cette solution est évidemment inacceptable car les clés stockées dans l'ordinateur peuvent être lues par un pirate à travers le réseau de communication et le même pirate pourrait utiliser à distance l'ordinateur pour calculer une signature sur un message que le propriétaire de l'ordinateur ne souhaiterait pas  
25 signer.

Il est donc souhaitable de pouvoir disposer d'un moyen sécurisé de traitement cryptographique qui, dans l'exemple de l'élaboration d'une signature, servirait au stockage de la clé privée du signataire et au calcul de la signature, le message restant stocké dans le moyen de  
30 stockage que constitue l'ordinateur par exemple.

Comme moyen sécurisé de traitement cryptographique, on peut utiliser une carte à microprocesseur, appelée aussi carte à puce. Dans

le cadre de la signature d'un message, la carte à puce offre les services suivants :

- stockage de la clé privée du signataire ;
- calcul de la réduction du message ;
- 5        - cryptage du message réduit.

Un exemple typique d'architecture d'implantation de cette application comprend essentiellement un ordinateur auquel est connecté la carte à puce par l'intermédiaire d'un boîtier. Du point de vue informatique, les opérations se déroulent de la manière suivante :

- 10        - stockage du message dans un moyen de stockage de l'ordinateur ;
- édition du message sur l'ordinateur ;
- calcul du message réduit sur la carte à puce ;
- cryptage du message réduit par la carte, après vérification du
- 15        code confidentiel introduit par le signataire au moyen du boîtier ;
- envoi du message et de la signature par la carte à l'ordinateur pour communication au réseau.

Avec ce système, le signataire est sûr que personne d'autre que lui  
20 ne peut utiliser sa clé privée pour signer. Cette solution est couramment utilisée et est suffisante pour un calcul de signature dont la portée ne vaut pas valeur légale, mais pour sécuriser un ensemble fermé d'ordinateurs, comme les réseaux internes de grandes entreprises.

25        Toutefois, on remarquera que le système de traitement cryptographique qui vient d'être décrit présente un certains nombres d'inconvénients :

- Le signataire n'est pas sûr du message qu'il signe puisqu'il n'est pas garanti qu'un virus dans l'ordinateur n'a pas modifié le
- 30        message avant l'opération de réduction ;
- Le destinataire n'est pas sûr que la vérification est bien effectuée sur le message reçu puisqu'il n'est pas garanti qu'un



virus dans l'ordinateur n'a pas fait apparaître le message correctement à l'écran alors que le message signé n'est pas celui visionné ;

- 5           - Le destinataire n'est pas sûr du résultat de la vérification puisqu'il n'est pas garanti qu'un virus dans l'ordinateur ne fait apparaître toute signature comme vérifiée alors qu'elle est fausse.

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de vérification de signature d'un  
10 message, le message, la signature, et un certificat ayant été envoyés par un signataire possédant une clef publique à un destinataire possédant un moyen de stockage de message, qui permette de remédier aux inconvénients des systèmes connus de traitement cryptographique, de manière à atteindre un niveau de sécurisation propre à conférer au  
15 message envoyé une valeur juridique incontestable et de manière à ce qu'un destinataire puisse vérifier l'identité du signataire et afin que ce dernier ne puisse révoquer le message qu'il a envoyé.

La solution au problème technique posé consiste, selon la présente invention, en ce que le procédé de vérification comporte les étapes selon  
20 lesquelles :

- on charge le message, la signature et le certificat, à partir du moyen de stockage dans un moyen sécurisé connecté audit moyen de stockage du destinataire,
- on vérifie le certificat dans le moyen sécurisé au moyen d'une  
25 clef publique d'un tiers de confiance associée audit certificat, et on transmet à un moyen de visualisation connecté directement au moyen sécurisé au moins une donnée de résultat de vérification,
- on vérifie la donnée de résultat sur le moyen de visualisation,
- 30 - lorsque le certificat est vérifié, on calcule dans le moyen sécurisé une réduction du message, et on recopie le message

sur le moyen de visualisation au fur et à mesure de l'opération de réduction,

- on déchiffre dans ledit moyen sécurisé la signature avec la clé publique du signataire,
- 5       - on compare la signature déchiffrée avec la réduction effectuée, et,
- selon le résultat de la comparaison, on envoie un message, du moyen sécurisé au moyen de visualisation, indiquant que la signature est conforme ou non au message ou à la clé publique
- 10       du signataire présentés.

Ainsi, on comprend qu'avec le procédé de vérification conforme à l'invention, le destinataire d'un message signé pourra avoir l'assurance que l'identité du signataire est authentique et que le message est intègre et ne pourra pas être révoqué puisqu'il verra apparaître sur le moyen de visualisation, un donnée de résultat de vérification du certificat, éventuellement le certificat, le message sur lequel la vérification de signature est effectuée, et le résultat de vérification de la signature, et, ceci sans que ces éléments ne circulent dans le moyen de stockage « non sûr », ordinateur par exemple, susceptible d'attaque frauduleuse,

15       la fonction de visualisation (impression, affichage ou archivage) étant un environnement fermé considéré comme « sûr ».

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

25       La figure 1 est un schéma en perspective d'un dispositif d'authentification utilisé par un procédé conforme à l'invention.

La figure 2 est bloc-diagramme du dispositif d'authentification de la figure 1.

Le dispositif d'authentification représenté sur la figure 1 est destiné à authentifier un message lors d'une opération de traitement cryptographique dudit message.

30

Dans la suite de cette description, on envisagera deux types de traitement cryptographique, à savoir la signature d'un message à envoyer à un destinataire et, inversement, la vérification par un destinataire de la signature d'un message reçu. Bien entendu, d'autres  
5 opérations de traitement cryptographique peuvent être mises en oeuvre au moyen de dispositif d'authentification de la figure 1, telles que le cryptage du message lui-même.

D'une manière générale, le dispositif d'authentification de message de la figure 1 comporte un moyen de stockage dudit message, constitué  
10 par exemple, par une mémoire dans l'unité centrale 11 d'un ordinateur 10. En fait, le message stocké est celui que l'auteur dudit message a composé au moyen du clavier 12 et qui doit faire l'objet d'une signature électronique. Normalement, le message composé apparaît sur l'écran 13 de l'ordinateur 10. L'unité centrale 11 communique avec l'extérieur,  
15 notamment avec les réseaux de communication, au moyen d'un câble 14 par lequel transitent les messages à signer et à envoyer ou les messages signés reçus.

L'unité centrale 11 est reliée par un câble 15 de liaison à un moyen sécurisé 21 de traitement cryptographique, ici constitué par une carte à  
20 microprocesseur disposée dans un boîtier 22. Comme le montre la figure 2, ledit boîtier 22 comprend un circuit 221 d'interface appelé circuit de commandes/données. Le message devant être signé ou le message dont la signature doit être vérifiée, ainsi que les données nécessaires aux opérations de signature ou de vérification, arrivent du  
25 moyen 11 de stockage à la carte 21 à puce par ce circuit en respectant par exemple la norme ISO 7816. Le circuit 221 de commandes/données dispose d'une entrée permettant de recevoir en actionnant un bouton 222 un signal de déclenchement de l'opération de signature et les données sur un clavier 224 du boîtier, comme par exemple un code  
30 confidentiel.

D'autre part, la carte 21 à puce est connectée directement à un moyen 30 de visualisation, ici une imprimante mais qui pourrait être

5 tout aussi bien un écran ou un moyen d'archivage, de manière à pouvoir transmettre au moins le message reçu de l'unité centrale 11, lors de l'opération du traitement cryptographique. La liaison entre la carte 21 à puce et l'imprimante 30 est réalisée par une interface 223 de visualisation du boîtier 22 par lequel passeront le message, et d'autres données devant être authentifiées.

10 L'architecture du dispositif d'authentification représentée aux figures 1 et 2 est donc basée sur une carte 21 à puce faisant le pont entre une zone « non sûre », l'ordinateur 10, et une zone « sûre », l'imprimante 30, la carte elle-même étant réputée « très sûre ».

15 Les entrées/sorties des circuits de commandes/données 221 et de visualisation 223 sont électriquement indépendantes lorsqu'aucune carte à puce n'est présente dans le boîtier 22. Lorsqu'une carte 21 est insérée dans le boîtier 22, la masse électrique est alors partagée entre les deux circuits 221 et 223. Les données issues de la carte 21 vers le circuit 223 de visualisation sortent par une sortie  $O_2$  spécifique et physiquement distincte de la sortie  $O_1$  utilisée pour le transfert des commandes/données. De même, les entrées  $I_1$  et  $I_2$  de commandes/données et de visualisation de la carte 21 sont  
20 physiquement distinctes. En fait, le seul lien logique entre les données circulant dans les circuits de commandes/données 221 et de visualisation 223 est le logiciel de la carte, réputé « très sûr ».

25 Dans le cas où la liaison entre la carte 21 à puce et l'imprimante 30 n'apparaîtrait pas suffisamment sécurisée, du fait notamment de son cheminement, il est prévu que la carte 21 puisse transmettre à l'imprimante 30 le message à traiter, et d'autres données, sous forme cryptée. Le mécanisme utilisé sera par exemple un algorithme symétrique, comme le triple DES, dont la clé peut être fixée ou négociée entre la carte 21 et le moyen 30 de visualisation.

30 Le déroulement d'une opération de signature d'un message est le suivant :

1. Le message à signer est édité dans le moyen 11 de stockage de l'ordinateur 10 et, éventuellement apparaît sur l'écran 13, puis le signataire demande à l'ordinateur de démarrer l'opération de signature.

2. L'ordinateur 10 transmet le message à la carte 21 via le circuit 221 de commandes/données par paquets de N octets afin d'être réduit par un algorithme de hachage ( $N = 64$  si l'algorithme SHA1 est employé).

3. Lors de l'initialisation de l'algorithme de hachage, le logiciel 211 de la carte 21 envoie une commande d'initialisation du moyen 30 de visualisation qui permettra d'authentifier le message de manière sûre.

4. Lors de l'arrivée du message venant du moyen 11 de stockage, le logiciel 211 de la carte 21 en calcule en ligne la réduction et le recopie sur la sortie  $O_2$  de visualisation, si bien que le moyen 30 de visualisation pourra faire apparaître, ici imprimer, le message au fur et à mesure de l'opération de réduction.

5. Lorsque la totalité du message a été envoyée à la carte 21 à puce par l'ordinateur, et avant d'effectuer l'opération de cryptage du message réduit, la carte se met en attente de réception d'un message de commande.

6. Le signataire a le temps d'authentifier le message imprimé, puis, s'il en accepte le contenu, compose ledit message de commande sous forme d'un code confidentiel saisi sur le clavier 224 du boîtier 22. Le circuit 221 de commandes/données génère lui-même la commande de l'opération de cryptage du message réduit en présentant la commande et le code confidentiel entré sur le clavier 224 par le signataire. L'ordinateur ne peut pas voir le contenu de cette commande. On pourra aussi disposer d'une entrée physiquement distincte sur la carte 21 à puce pour rentrer le code confidentiel.

7. La carte 21 à puce calcule la signature, renvoie la valeur à l'ordinateur 10 et, au besoin, au moyen 30 de visualisation. Le logiciel 211 de la carte 21 pourra aussi inclure d'autres données à visualiser,

telles que et non limitativement le numéro de série de la carte, le nom du signataire, etc, si ces données sont présentes dans la carte 21.

Il est important de noter que l'opération de signature ne pourra être activée sur la carte 21 que suite à une réduction et l'entrée du code confidentiel en tant que message de commande du cryptage du message réduit. De plus, suite au calcul de signature, l'autorisation de signature est effacée, obligeant ainsi à entrer le code confidentiel volontairement pour toute opération de signature ultérieure.

S'agissant d'une opération de vérification de la signature d'un message, le message et sa signature sont envoyés au destinataire, dans l'unité centrale 11 de son ordinateur 10. Le destinataire désirera alors vérifier l'authenticité de la signature par rapport au message et au signataire. On se placera ici dans le cas où le certificat du signataire est également envoyé au destinataire.

Le destinataire doit effectuer deux types de vérification. D'une part, la vérification du lien entre l'identité du signataire et la clé publique de vérification, c'est-à-dire la vérification du certificat, et, d'autre part, la vérification de la valeur de la signature par rapport au message reçu et au certificat.

La séquence se déroule comme suit:

1. Le destinataire déclenche l'opération de vérification par le chargement dans la carte 21 à puce du certificat du signataire et de la clé publique du tiers de confiance qui a issu le certificat.
2. L'ordinateur 10 demande la vérification du certificat avec la clé publique du tiers de confiance. Cette commande déclenche l'initialisation du moyen 30 de visualisation par la carte.
3. La carte 21 vérifie le certificat et transmet au moyen 30 de visualisation, via le circuit 223 de visualisation, les données suivantes: validité du certificat (avec les dates), clé publique du tiers de confiance utilisée pour vérifier le certificat, clé publique du signataire, nom du signataire, et d'autres données pouvant

- être liées au contexte d'utilisation. Ainsi, un destinataire recevant un faux certificat, numériquement intègre mais issu par un faux tiers de confiance, s'en apercevrait d'une manière sûre en comparant la valeur visualisée de la clé publique du «faux tiers» avec celle du «vrai tiers» dont la clé publique est publiée notoirement. Ainsi, le destinataire peut authentifier l'identité du signataire, et, grâce à une date de validité du certificat, peut être sûr de la date à laquelle un signataire a signé le message et de la non obsolescence dudit certificat. On peut également avoir une donnée transmise, au moyen 30 de visualisation, qui est un message disant que le certificat est bon ou mauvais. Dans ce cas, le destinataire vérifie juste le message et en déduit qu'il a reçu un faux ou un vrai certificat. Dans un autre exemple, si le certificat est juste, on peut transmettre le certificat au moyen 30 de visualisation, le destinataire compare alors le certificat visualisé avec le certificat envoyé.
4. Lorsque le certificat est vérifié, l'ordinateur 10 déclenche la commande de l'opération de réduction et envoie le message à la carte 21.
5. Lors de l'arrivée du message venant du moyen 11 de stockage, le logiciel 211 de la carte en calcule en ligne la réduction et le recopie sur la sortie O<sub>2</sub> de visualisation, si bien que le moyen 30 de visualisation fera apparaître, ici imprimer, le message au fur et à mesure de l'opération de réduction. Le destinataire peut ainsi vérifier que le message dont la réduction est calculée est bien intègre.
6. Lorsque la totalité du message a été envoyée à la carte 21 à puce par l'ordinateur 10, ce dernier demande alors la vérification de signature. Il passe en paramètre la valeur de la signature reçue du signataire. Le logiciel 211 de la carte déchiffre la signature avec la clé publique du signataire et la compare avec le résultat de la réduction effectuée en étape 5.

S'il y a égalité, la carte 21 envoie un message à l'ordinateur 10, indiquant que la signature est conforme au message et à la clé publique du certificat présenté. La carte envoie au circuit 223 de visualisation le message «Signature OK. Fin de vérification»,  
5 qui est visible par le vérificateur. Si la signature n'est pas exacte, alors la carte envoie un message à l'ordinateur, indiquant que la signature est non conforme au message ou à la clé publique du certificat présenté. La carte envoie au circuit 223 de visualisation le message «Signature inexacte. Fin de  
10 vérification», qui est visible par le vérificateur.

Ainsi, par ce procédé, le signataire pourra difficilement révoquer un message qu'il a lui-même envoyé.

L'ensemble de ces actions doit se dérouler dans l'ordre indiqué sans incident, sinon, la séquence est annulée par la carte 21 à puce et il  
15 est nécessaire de tout recommencer.

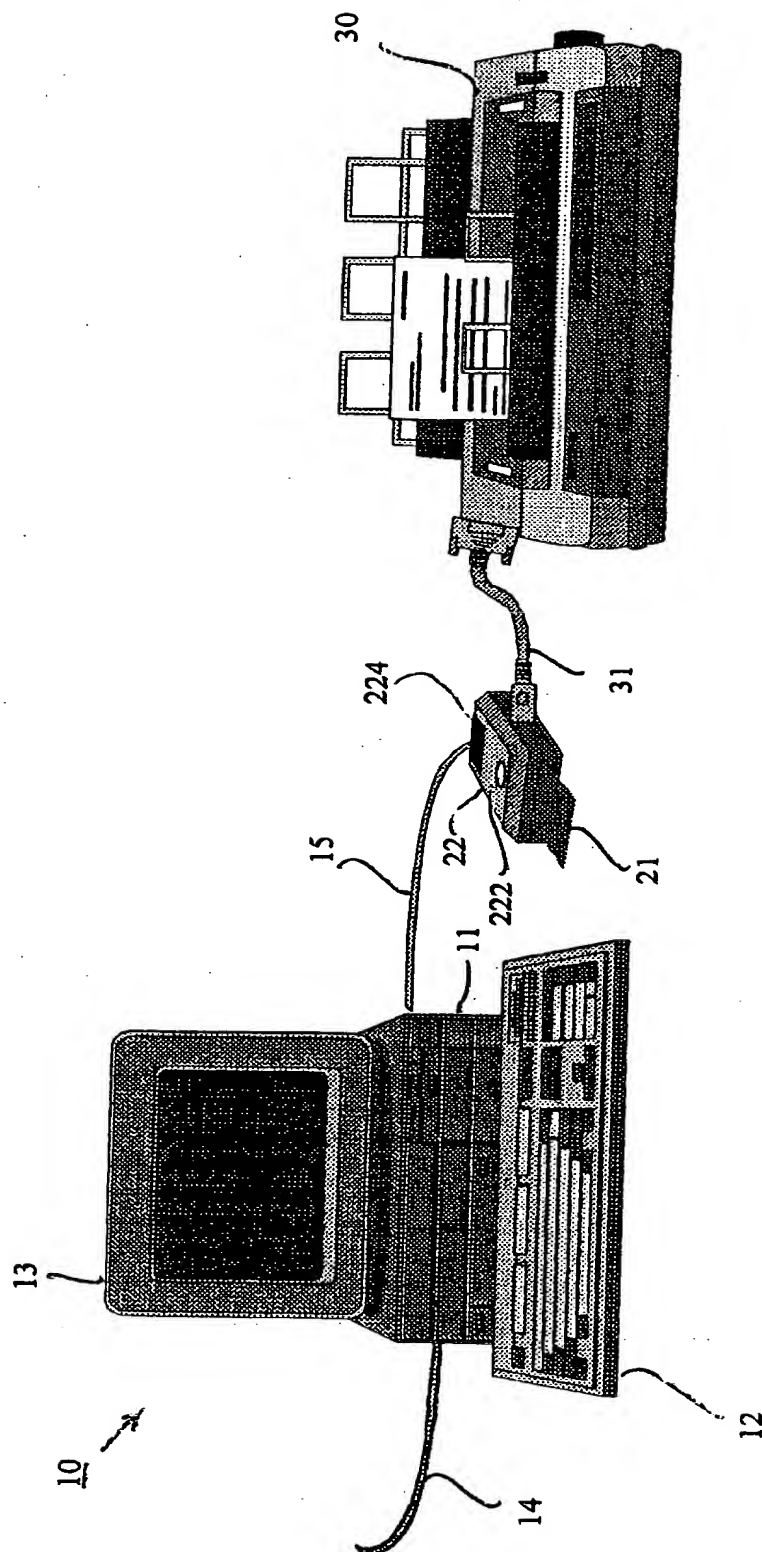
Bien entendu, les envois ou chargements du message, du certificat et de la signature peuvent se faire simultanément préalablement à la vérification du certificat. De même, les envois de commandes de vérification du certificat, d'opération de réduction et de vérification de  
20 signature peuvent se faire au moyen d'une unique commande. Cette unique commande peut comprendre le message, le certificat et la signature. Par suite, le logiciel de la carte identifie cette unique commande et l'exécute en conséquence. Bien entendu, préférentiellement la clef publique du signataire est également chargée  
25 dans la carte 21 à puce lors du chargement du certificat. Dans le cas contraire, elle se trouve déjà dans la carte.



## REVENDICATIONS

1. Procédé de vérification de signature d'un message, le message, la signature, et un certificat ayant été envoyés par un signataire possédant une clef publique à un destinataire possédant un moyen (11) de stockage de message, caractérisé en ce qu'il comporte les étapes selon lesquelles :
  - on charge le message, la signature et le certificat, à partir du moyen de stockage (11) dans un moyen sécurisé (21) connecté audit moyen de stockage (11) du destinataire,
  - on vérifie le certificat dans le moyen sécurisé (21) au moyen d'une clef publique d'un tiers de confiance associée audit certificat, et on transmet à un moyen (30) de visualisation connecté directement au moyen sécurisé (21) au moins une donnée de résultat de vérification,
  - on vérifie la donnée de résultat sur le moyen de visualisation (30),
  - lorsque le certificat est vérifié, on calcule dans le moyen sécurisé (21) une réduction du message, et on recopie le message sur le moyen (30) de visualisation au fur et à mesure de l'opération de réduction,
  - on déchiffre dans ledit moyen sécurisé (21) la signature avec la clé publique du signataire,
  - on compare la signature déchiffrée avec la réduction effectuée, et,
  - selon le résultat de la comparaison, on envoie un message, du moyen sécurisé (21) au moyen de visualisation (30), indiquant que la signature est conforme ou non au message ou à la clé publique du signataire présentés.
2. Procédé de vérification selon la revendication 1, caractérisé en ce que lors du chargement du certificat, on charge la clé publique du tiers de confiance.

- 5       **3.** Procédé de vérification selon l'une des revendications précédentes, caractérisé en ce que ledit moyen sécurisé (21) est constitué par une carte à microprocesseur disposée dans un boîtier (22) connecté, d'une part, audit moyen (11) de stockage, et, d'autre part, audit moyen (30) de visualisation.
- 10       **4.** Procédé de vérification selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit moyen (30) de visualisation est une imprimante, un écran ou un moyen d'archivage.
- 15       **5.** Procédé de vérification selon l'une quelconque des revendications précédentes, caractérisé en ce que, ledit moyen (21) sécurisé transmet audit moyen (30) de visualisation des données de résultat dudit certificat telles que la date de validité du certificat.
- 20       **6.** Procédé de vérification selon l'une quelconque des revendications précédentes, caractérisé en ce que le moyen sécurisé (21) comporte, d'une part, un circuit d'interface de commandes/données (221) réalisant une liaison avec le moyen (11) de stockage, et d'autre part, un circuit d'interface de visualisation (223) réalisant une liaison avec le moyen (30) de visualisation, lesdits circuits étant physiquement indépendants.



**Figure 1**

**THIS PAGE BLANK (USPTO)**

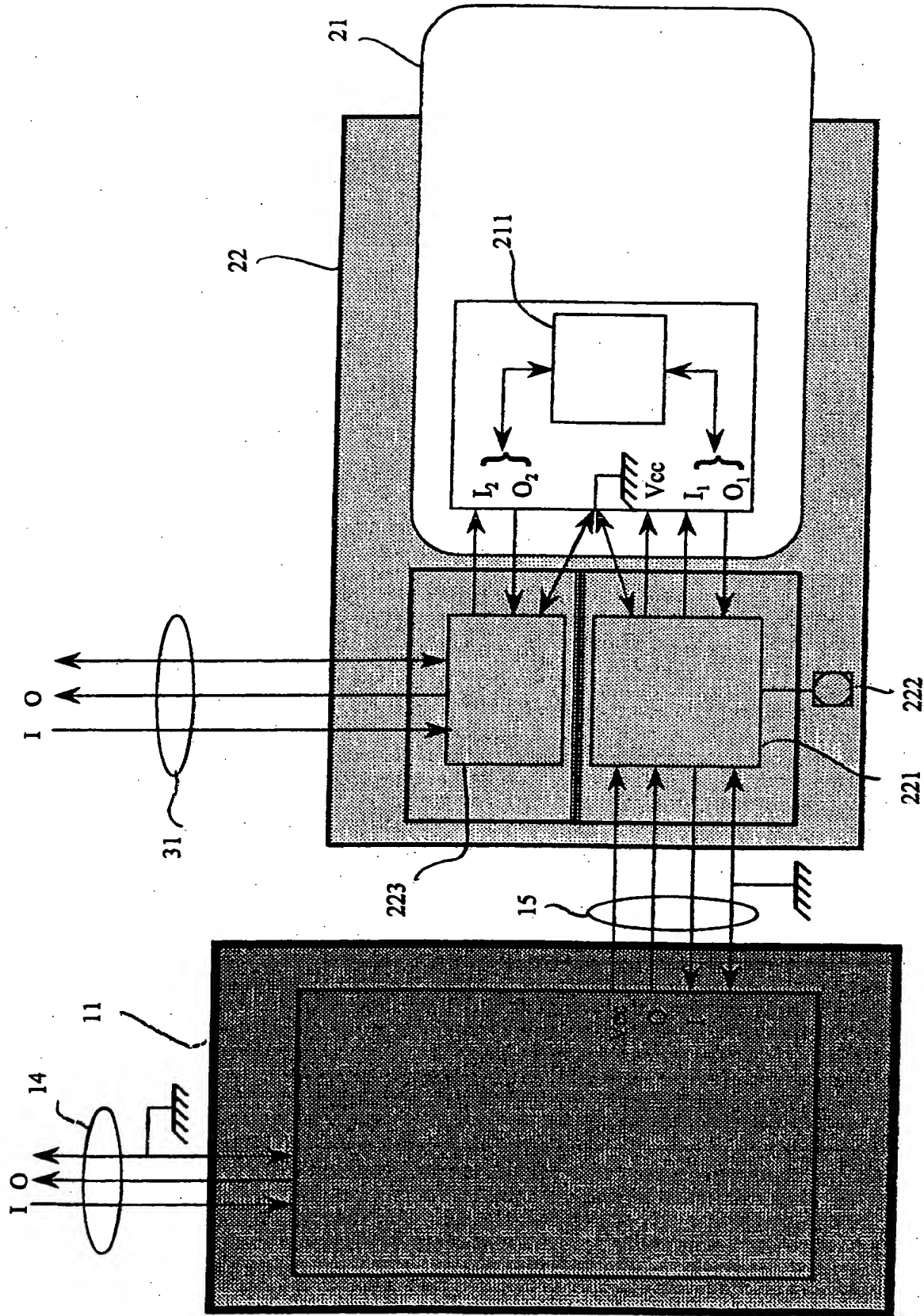


Figure 2

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/00679

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 08415 A (SEDLAK HOLGER ;SIEMENS AG (DE)) 18 February 1999 (1999-02-18) page 2, line 22 - line 34 page 4, line 4 - line 16	1-6
A	PRENEEL B: "CRYPTOGRAPHIC HASH FUNCTIONS" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, vol. 5, no. 4, 1 July 1994 (1994-07-01), pages 17-34, XP000460559 ISSN: 1120-3862 page 29, column 2, last line -page 30, column 2	1-6
A	EP 0 785 514 A (SOLAIC SA) 23 July 1997 (1997-07-23) column 2, line 48 -column 4, line 39	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \* & \* document member of the same patent family

Date of the actual completion of the international search

4 May 2000

Date of mailing of the international search report

15/05/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Zucka, G

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/FR 00/00679

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9908415	A	18-02-1999	NONE	
EP 0785514	A	23-07-1997	FR 2743910 A	25-07-1997
			JP 9305568 A	28-11-1997
			US 5894550 A	13-04-1999



# RAPPORT DE RECHERCHE INTERNATIONALE

Denominazione internazionale No

PCT/FR 00/00679

### A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

## B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

### C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 99 08415 A (SEDLAK HOLGER ;SIEMENS AG (DE)) 18 février 1999 (1999-02-18) page 2, ligne 22 - ligne 34 page 4, ligne 4 - ligne 16	1-6
A	PRENEEL B: "CRYPTOGRAPHIC HASH FUNCTIONS" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, vol. 5, no. 4, 1 juillet 1994 (1994-07-01), pages 17-34, XP000460559 ISSN: 1120-3862 page 29, colonne 2, dernière ligne -page 30, colonne 2	1-6

—  
-/-

**X**

Voilà la suite du cadre C pour la fin de la liste des documents

☒

**Les documents de familles de brevets sont indiqués en annexe**

• Catégories spéciales de documents cités:

\*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent

\*E document antérieur, mais publié à la date de dépôt international ou après cette date

\*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

**"T"** document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

**"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément**

**"Y"** document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

\*8\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

**4 mai 2000**

**Date d'expédition du présent rapport de recherche internationale**

**15/05/2000**

Norm et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

**Zucka, G**

# RAPPORT DE RECHERCHE INTERNATIONALE

Den ☐ Internationale No  
PCT/FR 00/00679

## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>EP 0 785 514 A (SOLAIC SA)  23 juillet 1997 (1997-07-23)  colonne 2, ligne 48.-colonne 4, ligne 39</p>	1

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den e Internationale No

PCT/FR 00/00679

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9908415 A	18-02-1999	AUCUN	
EP 0785514 A	23-07-1997	FR 2743910 A	25-07-1997
		JP 9305568 A	28-11-1997
		US 5894550 A	13-04-1999

**THIS PAGE BLANK (USPTO)**

# PCT

## RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire <b>76.0569</b>	<b>POUR SUITE</b> voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après <b>A DONNER</b>	
Demande internationale n° <b>PCT/FR 00/00679</b>	Date du dépôt international (jour/mois/année) <b>17/03/2000</b>	(Date de priorité (la plus ancienne) (jour/mois/année) <b>17/03/1999</b>
Déposant  <b>SCHLUMBERGER SYSTEMES et al.</b>		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

**1. Base du rapport**

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

**4. En ce qui concerne le titre,**

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

**5. En ce qui concerne l'abrégé,**

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

**6. La figure des dessins à publier avec l'abrégé est la Figure n°**

- ☒ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

1  
☐ Aucune des figures n'est à publier.

**THIS PAGE BLANK (USPTO)**

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 99 08415 A (SEDLAK HOLGER ; SIEMENS AG (DE)) 18 février 1999 (1999-02-18) page 2, ligne 22 - ligne 34 page 4, ligne 4 - ligne 16	1-6
A	PRENEEL B: "CRYPTOGRAPHIC HASH FUNCTIONS" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, vol. 5, no. 4, 1 juillet 1994 (1994-07-01), pages 17-34, XP000460559 ISSN: 1120-3862 page 29, colonne 2, dernière ligne -page 30, colonne 2	1-6

☒ Voir la suite du cadre C pour la fin de la liste des documents☒ Les documents de familles de brevets sont indiqués en annexe

## \* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

4 mai 2000

Date d'expédition du présent rapport de recherche internationale

15/05/2000

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Zucka, G

**THIS PAGE BLANK (USPTO)**



## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	✓ EP 0 785 514 A (SOLAIC SA) 23 juillet 1997 (1997-07-23) colonne 2, ligne 48 - colonne 4, ligne 39 -----	1

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/00679

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9908415	A	18-02-1999	NONE	
EP 0785514	A	23-07-1997	FR 2743910 A	25-07-1997
			JP 9305568 A	28-11-1997
			US 5894550 A	13-04-1999

**THIS PAGE BLANK (USPTO)**

**RAPPORT DE RECHERCHE INTERNATIONALE**

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/FR 00/00679

7 6 0 5 6 9

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9908415 A	18-02-1999	AUCUN	
EP 0785514 A	23-07-1997	FR 2743910 A	25-07-1997
		JP 9305568 A	28-11-1997
		US 5894550 A	13-04-1999

**THIS PAGE BLANK (USPTO)**

RAPPORT DE RECHERCHE  
PRELIMINAIREétabli sur la base des dernières revendications  
déposées avant le commencement de la rechercheN° d'enregistrement  
nationalFA 574881  
FR 9903330

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 99 08415 A (SEDLAK HOLGER ; SIEMENS AG (DE)) 18 février 1999 (1999-02-18) * page 2, ligne 22 - ligne 34 * * page 4, ligne 4 - ligne 16 *	1-14
A	PRENEEL B: "CRYPTOGRAPHIC HASH FUNCTIONS" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, vol. 5, no. 4, 1 juillet 1994 (1994-07-01), pages 17-34, XP000460559 ISSN: 1120-3862 * page 29, colonne 2, dernière ligne - page 30, colonne 2 *	1-14
A	EP 0 785 514 A (SOLAIC SA) 23 juillet 1997 (1997-07-23) * colonne 2, ligne 48 - colonne 4, ligne 39 *	1
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		H04L
Date d'achèvement de la recherche		Examineur
2 novembre 1999		Zucka, G
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons &amp; : membre de la même famille, document correspondant</p>		

**THIS PAGE BLANK (USPTO)**



**ANNEXE AU RAPPORT DE RECHERCHE PRELIMINAIRE  
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO.**

FA 574881  
FR 9903330

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.  
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du  
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets,  
ni de l'Administration française

02-11-1999

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9908415      A	18-02-1999	AUCUN	
EP 0785514      A	23-07-1997	FR    2743910 A	25-07-1997
		JP    9305568 A	28-11-1997
		US    5894550 A	13-04-1999

**THIS PAGE BLANK (USPTO)**